T S9/5/1

9/5/1
DIALOG(R)File 347:JAPIO

06124401 **Image available**
PORTABLE ELECTRONIC DEVICE AND ACCESS MANAGING METHOD FOR THE SAME

PUB. NO.: 11-065938 [JP 11065938 A]
PUBLISHED: March 09, 1999 (19990309)
INVENTOR(s): IIJIMA YASUO
APPLICANT(s): TOSHIBA CORP
APPL. NO.: 09-286930 [JP 97286930]
FILED: October 20, 1997 (19971020)
INTL CLASS: G06F-012/14; G06K-019/073

ABSTRACT

PROBLEM TO BE SOLVED: To provide a portable electronic device and an access managing method for the same with which certificate information different for each file can be used, access conditions can be changed for each file and each area and further the leak of certificate information can be prevented.

SOLUTION: Plural pieces of key data (password numbers) are stored in a data memory, these key data are collated with key data selectively inputted from the outside, and this collated result is stored for each piece of key data. In the case of access to the area of a data memory, when any one of the respective stored collated results is positive, access is enabled. When all the respective stored collated results are positive, access is enabled and it is set for each piece of instruction data for accessing the respective areas of the data memory.

?

(19)日本国特許庁（ＪＰ）　(12) 公開特許公報（A）　(11)特許出願公開番号

特開平11－65938

(43)公開日　平成11年(1999)３月９日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ０６Ｆ　12/14	３２０	Ｇ０６Ｆ　12/14	３２０Ｃ
Ｇ０６Ｋ　19/073		Ｇ０６Ｋ　19/00	Ｐ

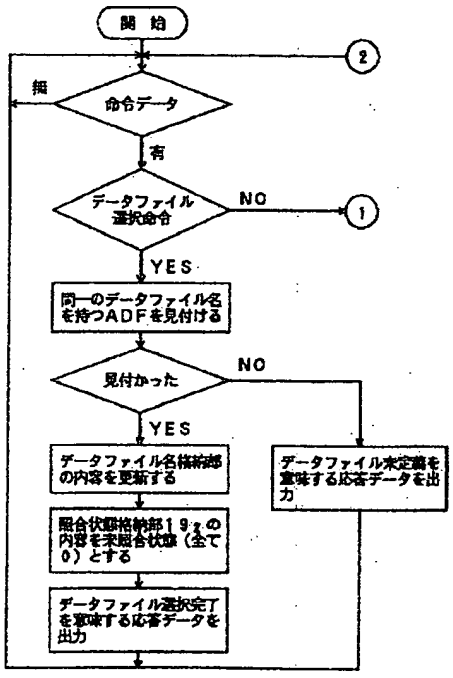
審査請求　有　　請求項の数７　ＯＬ　（全 12 頁）

(21)出願番号　特願平9－286930
(62)分割の表示　特願昭63－211834の分割
(22)出願日　昭和63年(1988)８月26日

(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地
(72)発明者　飯島　康雄
神奈川県川崎市幸区柳町70番地　株式会社東芝柳町工場内
(74)代理人　弁理士　鈴江　武彦　（外６名）

(54)【発明の名称】　携帯可能電子装置および携帯可能電子装置におけるアクセス管理方法

(57)【要約】
【課題】ファイルごとに異なる認証情報を用いることができるとともに、ファイルごと、および、エリアごとにアクセス条件を変えることができ、しかも、認証情報の漏洩を防止することができる携帯可能電子装置および携帯可能電子装置におけるアクセス管理方法を提供する。
【解決手段】データメモリ内に複数のキーデータ（暗証番号）を記憶しておき、これらキーデータを選択的に外部から入力されるキーデータと照合し、この照合結果を上記各キーデータごとに記憶しておき、データメモリのエリアに対してのアクセスの際、上記記憶してある各照合結果のうちいずれか１つが肯定的となっているときアクセス可能とし、上記記憶してある各照合結果の全てが肯定的となっているときアクセス可能とし、かつ、それらをデータメモリの各エリアに対するアクセスのための命令データごとに設定できるようにしている。



1

【特許請求の範囲】

【請求項１】　複数のファイルを有するメモリ部と、このメモリ部に対してアクセスを行なうための制御部を有し、選択的に外部とのデータの入出力を行なう携帯可能電子装置において、

前記各ファイルにはファイル名が付与されていて、各ファイルには複数のエリアと、ファイル内のエリアへのアクセスのために用いる複数の認証情報を記憶する認証情報記憶部が設けられており、かつ、各エリアには該エリアへのアクセスの際に必要な認証情報を示す照合状態確認情報およびこの照合状態確認情報にて示されている認証情報の組合わせをアンド論理とするかオア論理とするかの識別情報が記憶されており、

外部からファイル名を指定するファイル選択命令を受信した場合、前記各ファイルに付与されているファイル名に基づいてファイルを選択するファイル選択手段と、

外部から認証情報の照合命令を受信した場合、前記選択手段にて選択されているファイル内に記憶されている認証情報と照合命令とともに外部から供給された認証情報とを照合する照合手段と、

この照合手段による照合の結果を前記複数の認証情報ごとに保持する保持手段と、

前記複数のエリアへのアクセスの際に前記識別情報に基づき前記照合状態確認情報にて示されている認証情報の組合わせがアンド論理であるのかオア論理であるのかを判定する第１の判定手段と、

この第１の判定手段によりアンド論理であると判定された場合、前記照合状態確認情報にて示されている認証情報の全てについての照合結果が肯定的であるかを前記保持手段に保持されている照合結果に基づいて判定する第２の判定手段と、

この第２の判定手段によりオア論理であると判定された場合、前記照合状態確認情報にて示されている認証情報のうちいずれか１つが肯定的であるかを前記保持手段に保持されている照合結果に基づいて判定する第３の判定手段と、

前記第２の判定手段および前記第３の判定手段による判定結果が肯定的である場合に前記エリアへのアクセスを行なう手段と、

を具備したことを特徴とする携帯可能電子装置。

【請求項２】　前記複数のエリアには該エリアへのアクセスの際に必要な第１組の認証情報を示す第１の照合状態確認情報および該エリアへのアクセスの際に必要な第２組の認証情報を示す第２の照合状態確認情報が記憶されており、外部から受信した命令に基づき前記複数のエリアのうちいずれかにアクセスを行なう際に、前記第１の照合状態確認情報を用いるか前記第２の照合状態確認情報を用いるかを各命令データごとに対応して記憶している対応テーブルを有し、

エリアへのアクセスの際には受信した命令データと前記

2

対応テーブルとに基づき前記第１の照合状態確認情報を用いるか前記第２の照合状態確認情報を用いるかを選択する選択手段を具備したことを特徴とする請求項１記載の携帯可能電子装置。

【請求項３】　前記照合状態確認情報にて認証情報が示されておらず、かつ、前記識別情報がアンド論理の場合には前記照合結果を判定することなく、エリアへのアクセスを不可とするアクセス禁止手段と、

前記照合状態確認情報にて認証情報が示されておらず、かつ、前記識別情報がオア論理の場合には前記照合結果を参照することなく、エリアへのアクセスを許可するアクセス許可手段と、

を具備したことを特徴とする請求項１記載の携帯可能電子装置。

【請求項４】　前記携帯可能電子装置は前記メモリ部を構成するデータメモリと前記制御部を構成する制御素子およびプログラムメモリとからなる１つのＩＣチップにより構成されていることを特徴とする請求項１記載の携帯可能電子装置。

【請求項５】　複数のファイルを有するメモリ部と、このメモリ部に対してアクセスを行なうための制御部を有し、選択的に外部とのデータの入出力を行なう携帯可能電子装置におけるアクセス管理方法において、

前記各ファイルにはファイル名が付与されていて、各ファイルには複数のエリアを設けるとともに、ファイル内のエリアへのアクセスのために用いる複数の認証情報を記憶し、かつ、各エリアには該エリアへのアクセスの際に必要な認証情報を示す照合状態確認情報およびこの照合状態確認情報にて示されている認証情報の組合わせをアンド論理とするかオア論理とするかの識別情報を記憶しておき、

外部からファイル名を指定するファイル選択命令を受信した場合、前記各ファイルに付与されているファイル名に基づいてファイルを選択し、

外部から認証情報の照合命令を受信した場合、前記選択されているファイル内に記憶されている認証情報と照合命令とともに外部から供給された認証情報とを照合し、

この照合の結果を前記複数の認証情報ごとに保持しておき、

前記複数のエリアへのアクセスの際に前記識別情報に基づき前記情報照合状態確認情報にて示されている認証情報の組合わせがアンド論理であるのかオア論理であるのかを判定する第１の判定ステップと、

この第１の判定ステップによりアンド論理であると判定された場合、前記照合状態確認情報にて示されている認証情報の全てについての照合結果が肯定的であるかを前記保持されている照合結果に基づいて判定する第２の判定ステップと、

前記第１の判定ステップによりオア論理であると判定された場合、前記照合状態確認情報にて示されている認証

情報のうちいずれか１つが肯定的であるかを前記保持されている照合結果に基づいて判定する第３の判定ステップと、
前記第２の判定ステップおよび前記第３の判定ステップによる判定結果が肯定的である場合に前記エリアへのアクセスを行なうステップと、
を具備したことを特徴とする携帯可能電子装置におけるアクセス管理方法。
【請求項６】前記複数のエリアには該エリアへのアクセスの際に必要な第１組の認証情報を示す第１の照合状態確認情報および該エリアへのアクセスの際に必要な第２組の認証情報を示す第２の照合状態確認情報が記憶されており、外部から受信した命令に基づき前記複数のエリアのうちいずれかにアクセスを行なう際に、前記第１の照合状態確認情報を用いるか前記第２の照合状態確認情報を用いるかを各命令データとに対応して記憶している対応テーブルを有し、
エリアへのアクセスの際には受信した命令データと前記対応テーブルに基づき前記第１の照合状態確認情報を用いるか前記第２の照合状態確認情報を用いるかを選択する選択ステップを具備したことを特徴とする請求項５記載の携帯可能電子装置におけるアクセス管理方法。
【請求項７】前記照合状態確認情報にて認証情報が示されておらず、かつ、前記識別情報がアンド論理の場合には前記照合結果を判定することなく、エリアへのアクセスを不可とし、前記照合状態確認情報にて認証情報が示されておらず、かつ、前記識別情報がオア論理の場合には前記照合結果を参照することなく、エリアへのアクセスを許可するようにしたとを特徴とする請求項５記載の携帯可能電子装置におけるアクセス管理方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、たとえば、不揮発性メモリおよびＣＰＵなどの制御素子を有するＩＣ（集積回路）チップを内蔵した、いわゆるＩＣカードと称される携帯可能電子装置、および、この携帯可能電子装置におけるアクセス管理方法に関する。
【０００２】
【従来の技術】近年、新たな携帯可能なデータ記憶媒体として、消去可能な不揮発性メモリおよびＣＰＵなどの制御素子を有するＩＣチップを内蔵した、いわゆるＩＣカードが開発されている。
【０００３】この種のＩＣカードは、内蔵するメモリに認証情報としての暗証番号が記憶されており、外部から暗証番号を入力することにより、メモリに記憶されている登録暗証番号とを内部で照合し、その照合結果に応じて以降のメモリのエリアに対するアクセスの可否を決定するようになっている。
【０００４】
【発明が解決しようとする課題】さて、ＩＣカードの多目的利用のためには、メモリ内に複数の暗証番号を記憶しておくことにより、メモリのエリアへのアクセスに必要な暗証番号の種々の組合せをエリアごとに設定でき、かつ、エリアへのアクセスとして、たとえば、読出し、書込みなどの命令データごとにも設定すれば、ＩＣカードシステムの構築において柔軟性が得られる。しかし、従来のＩＣカードではそれが不可能であった。このため、エリアへのアクセス条件がきめ細かく設定できず、ＩＣカードシステムの構築において柔軟性に欠けるという欠点があった。
【０００５】また、エリアに対するアクセスの可否を決定する方法として、メモリ内に複数の暗証番号を記憶しておくとともに、各エリアに対しどの暗証番号が照合されるとアクセス可能なのかを示す識別情報を各エリアごとに対応させて記憶しておくことにより、アクセスのたびに暗証番号の照合結果と上記識別情報とを比較してアクセスの可否を決定することが考えられる。しかし、上記識別情報が全てのアクセス命令データに共通に使用されるとしたら、全ての命令データに対するアクセス条件が同一となり、運用しにくくなる。
【０００６】そこで、本発明は、ファイルごとに異なる認証情報を用いることができるとともに、ファイルごと、および、エリアごとにアクセス条件を変えることができ、しかも、認証情報の漏洩を防止することができる携帯可能電子装置および携帯可能電子装置におけるアクセス管理方法を提供することを目的とする。
【０００７】
【課題を解決するための手段】本発明の携帯可能電子装置は、複数のファイルを有するメモリ部と、このメモリ部に対してアクセスを行なうための制御部を有し、選択的に外部とのデータの入出力を行なう携帯可能電子装置において、前記各ファイルにはファイル名が付与されていて、各ファイルには複数のエリアと、ファイル内のエリアへのアクセスのために用いる複数の認証情報を記憶する認証情報記憶部が設けられており、かつ、各エリアには該エリアへのアクセスの際に必要な認証情報を示す照合状態確認情報およびこの照合状態確認情報にて示されている認証情報の組合わせをアンド論理とするかオア論理とするかの識別情報が記憶されており、外部からファイル名を指定するファイル選択命令を受信した場合、前記各ファイルに付与されているファイル名に基づいてファイルを選択するファイル選択手段と、外部から認証情報の照合命令を受信した場合、前記選択手段にて選択されているファイル内に記憶されている認証情報と照合命令とともに外部から供給された認証情報とを照合する照合手段と、この照合手段による照合の結果を前記複数の認証情報ごとに保持する保持手段と、前記複数のエリアへのアクセスの際に前記識別情報に基づき前記照合状態確認情報にて示されている認証情報の組合わせがアンド論理であるのかオア論理であるのかを判定する第１の

判定手段と、この第1の判定手段によりアンド論理であると判定された場合、前記照合状態確認情報にて示されている認証情報の全てについての照合結果が肯定的であるかを前記保持手段に保持されている照合結果に基づいて判定する第2の判定手段と、この第2の判定手段によりオア論理であると判定された場合、前記照合状態確認情報にて示されている認証情報のうちいずれか1つが肯定的であるかを前記保持手段に保持されている照合結果に基づいて判定する第3の判定手段と、前記第2の判定手段および前記第3の判定手段による判定結果が肯定的である場合に前記エリアへのアクセスを行なう手段とを具備したことを特徴とする。

【0008】また、本発明の携帯可能電子装置におけるアクセス管理方法は、複数のファイルを有するメモリ部と、このメモリ部に対してアクセスを行なうための制御部を有し、選択的に外部とのデータの入出力を行なう携帯可能電子装置におけるアクセス管理方法において、前記各ファイルにはファイル名が付与されていて、各ファイルには複数のエリアを設けるとともに、ファイル内のエリアへのアクセスのために用いる複数の認証情報を記憶し、かつ、各エリアには該エリアへのアクセスの際に必要な認証情報を示す照合状態確認情報およびこの照合状態確認情報にて示されている認証情報の組合わせをアンド論理とするかオア論理とするかの識別情報を記憶しておき、外部からファイル名を指定するファイル選択命令を受信した場合、前記各ファイルに付与されているファイル名に基づいてファイルを選択し、外部から認証情報の照合命令を受信した場合、前記選択されているファイル内に記憶されている認証情報と照合命令とともに外部から供給された認証情報とを照合し、この照合の結果を前記複数の認証情報ごとに保持しておき、前記複数のエリアへのアクセスの際に前記識別情報に基づき前記情報照合状態確認情報にて示されている認証情報の組合わせがアンド論理であるのかオア論理であるのかを判定する第1の判定ステップと、この第1の判定ステップによりアンド論理であると判定された場合、前記照合状態確認情報にて示されている認証情報の全てについての照合結果が肯定的であるかを前記保持されている照合結果に基づいて判定する第2の判定ステップと、前記第1の判定ステップによりオア論理であると判定された場合、前記照合状態確認情報にて示されている認証情報のうちいずれか1つが肯定的であるかを前記保持されている照合結果に基づいて判定する第3の判定ステップと、前記第2の判定ステップおよび前記第3の判定ステップによる判定結果が肯定的である場合に前記エリアへのアクセスを行なうステップとを具備したことを特徴とする。

【0009】本発明によれば、内部に複数の認証情報を記憶しておき、これら認証情報を選択的に外部から入力される認証情報と照合し、この照合結果を上記各認証情報ごとに記憶しておき、エリアに対してのアクセスの際、上記記憶してある各照合結果のうちいずれか1つが肯定的となっているときアクセス可能とし、上記記憶してある各照合結果の全てが肯定的となっているときアクセス可能とするものである。

【0010】これにより、各エリアごとにエリアへのアクセスに必要となる認証情報の組合せを任意に設定でき、しかも、その組合せに対して特にアンド論理あるいはオア論理を合せて設定できる。したがって、各エリアへのアクセス条件がきめ細かく設定でき、システム構築において柔軟性が得られるようになる。

【0011】すなわち、本発明によれば、ファイルごとに認証情報が記憶されているので、ファイルごとに異なる認証情報を用いることができる。また、ファイルごとの認証情報を用いてファイル内の各エリアのアクセス条件が記憶されているので、ファイルごと、および、エリアごとにアクセス条件を変えることができる。さらに、ファイルを選択していないと認証情報の照合が不可能となるので、認証情報の漏洩を防止することができる。

【0012】

【発明の実施の形態】以下、本発明の実施の形態について図面を参照して説明する。図14は、本発明に係る携帯可能電子装置としてのICカードを取扱う端末装置の構成例を示すものである。すなわち、この端末装置は、ICカード1をカードリーダ・ライタ2を介してCPUなどからなる制御部3と接続可能にするとともに、制御部3にキーボード4、CRTディスプレイ装置5、プリンタ6、および、フロッピィディスク装置7を接続して構成される。

【0013】ICカード1は、ユーザが保持し、たとえば、商品購入などの際にユーザのみが知得している暗証番号の参照や必要データの蓄積などを行なうもので、たとえば、図13にその機能ブロックを示すように、リード・ライト部11、暗証設定・暗証照合部12、および、暗号化・復号化部13などの基本機能を実行する部分と、これらの基本機能を管理するスーパバイザ14とで構成されている。

【0014】リード・ライト部11は、データメモリ16などに対してデータの読出し、書込み、あるいは消去を行なう機能である。暗証設定・暗証照合部12は、ユーザが設定した暗証番号の記憶および読出禁止処理を行なうとともに、暗証番号の設定後にその暗証番号の照合を行ない、以後の処理の許可を与える機能である。

【0015】暗号化・復号化部13は、たとえば、通信回線を介して制御部3から他の端末装置へデータを送信する場合の通信データの漏洩、偽造を防止するための暗号化や、暗号化されたデータの復号化を行なうものであり、たとえば、DES（Data Encryption Standard）など、充分な暗号強度を有する暗号化アルゴリズムにしたがってデータ処理を行なう機能である。

【００１６】スーパバイザ１４は、カードリーダ・ライタ２から入力された機能コード、もしくは、データの付加された機能コードを解読し、前記基本機能のうち必要な機能を選択して実行させる機能である。

【００１７】これらの諸機能を発揮させるために、ＩＣカード１は、たとえば、図１２に示すように、ＣＰＵなどの制御素子（制御部）１５、メモリ部としてのデータメモリ１６、プログラムメモリ１７、および、カードリーダ・ライタ２との電気的接触を得るためのコンタクト部１８によって構成されており、これらのうち制御素子１５、データメモリ１６、および、プログラムメモリ１７は１つのＩＣチップ（あるいは複数のＩＣチップ）で構成されてＩＣカード本体内に埋設されている。

【００１８】プログラムメモリ１７は、たとえば、マスクＲＯＭで構成されており、前記各基本機能を実現するサブルーチンを備えた制御素子１５の制御プログラムなどを記憶するものである。

【００１９】データメモリ１６は、各種データの記憶に使用され、たとえば、ＥＥＰＲＯＭなどの消去可能な不揮発性メモリで構成されている。そして、データメモリ１６は、たとえば、図４に示すように、全てのアプリケーションで運用する１つのコモンデータファイル２１と、アプリケーション個別に運用する複数（図では２つ）のアプリケーションデータファイル２２１，２２２とによって構成されており、それぞれのデータファイル２１，２２１，２２２には、複数の認証情報としてのキーデータ（暗証番号）が記憶されているとともに、複数のエリアが存在している。

【００２０】アプリケーションデータファイル２２１，２２２には、それぞれデータファイル名（ＤＦＮ）が付与されており、後述するデータファイル選択命令データを用いて、このデータファイル名を指定することにより、以降のアクセス対象となるアプリケーションデータファイルを認識するようになっている。

【００２１】各キーデータには、たとえば、図５に示すように、キーデータを指定する識別情報（ＫＩＤ）が付与されており、後述するキーデータ照合命令データを用いて、この識別情報を指定することにより、照合処理の対象となるキーデータを認識するようになっている。

【００２２】図４の例では、コモンデータファイル２１に属するキーデータ１，２，３に対して、それぞれＫＩＤ０１，ＫＩＤ０２，ＫＩＤ０３が付与されている。また、アプリケーションデータファイル２２１に属するキーデータＸ４，Ｘ５，Ｘ６に対して、それぞれＫＩＤ０４，ＫＩＤ０５，ＫＩＤ０６が付与されている。さらに、アプリケーションデータファイル２２２に属するキーデータＹ４，Ｙ５，Ｙ６に対しても、それぞれＫＩＤ０４，ＫＩＤ０５，ＫＩＤ０６が付与されている。

【００２３】また、各キーデータには、たとえば、図５に示すように、個別に照合状態指定情報が付与されており、以降のアクセスに必要となるキーデータが照合済となっているか否かの識別に使用される。

【００２４】キーデータが照合済であるか否かの情報は、図７に示す照合状態格納部２３１，２３２に格納される。この照合状態格納部２３１，２３２は、たとえば、制御素子１５に内蔵されたＲＡＭ内に設けられており、コモンデータファイル２１に属するキーデータの場合には照合状態格納部２３１に、また、アプリケーションデータファイル２２１，２２２に属するキーデータの場合には照合状態格納部２３２に、それぞれ格納される。

【００２５】また、図７に示すように、照合状態格納部２３１，２３２とともにデータファイル名格納部２４が設けられており、このデータファイル名格納部２４には、後述するデータファイル選択命令データによりアクセス対象として選択されたデータファイルのデータファイル名が格納される。

【００２６】一方、各エリアには、たとえば、図６に示すように、エリアを指定する識別情報（ＡＩＤ）が付与されており、後述するエリア処理命令データを用いて、この識別情報を指定することにより、エリア処理の対象となるエリアを認識するようになっている。

【００２７】図４の例では、コモンデータファイル２１に属するエリアＧ，Ｈに対して、それぞれＡＩＤｇｇ，ＡＩＤｈｈが付与されている。また、アプリケーションデータファイル２２１に属するエリアＡ，Ｂ，Ｃに対して、それぞれＡＩＤａａ，ＡＩＤｂｂ，ＡＩＤｃｃが付与されている。さらに、アプリケーションデータファイル２２２に属するエリアＤ，Ｅ，Ｆに対して、それぞれＡＩＤｄｄ，ＡＩＤｅｅ，ＡＩＤｆｆが付与されている。

【００２８】また、各エリアには、たとえば、図６に示すように、個別に第１，第２照合状態確認情報が付与されているとともに、これら第１，第２照合状態確認情報にはそれぞれ論理情報（ＡまたはＯ）が付与されている。第１，第２照合状態確認情報は、エリアアクセスの際に必要となるキーデータの照合状態を要求するものである。また、論理情報は、照合状態確認情報の組合せをアンド（ＡＮＤ）論理とするかオア（ＯＲ）論理とするかという識別情報であり、アンド論理の場合は「Ａ」、オア論理の場合は「Ｏ」となっている。

【００２９】図８は、各エリアに割当てられた２つの照合状態確認情報を命令コード別に選択するためのデータテーブルを示すもので、各種命令コードにそれぞれ対応して照合状態確認情報を選択するための選択情報が格納されており、このデータテーブルは、たとえば、データメモリ１６内に設けられている。

【００３０】次に、このような構成において、図１ないし図３に示すフローチャートを参照しつつ動作を説明する。なお、フローチャート上では、コモンデータファイル２１をＣＤＦ、アプリケーションデータファイル２２

1，222をADFと略記する。

【0031】まず、データファイルの選択処理を説明する。定常状態においては、命令データ待ち状態になっており、この状態で命令データが入力されると、制御素子15は、図9に示すようなデータファイル選択命令データか否かを判断する。この判断の結果、データファイル選択命令データでなければ、制御素子15は別の処理を行なう。

【0032】上記命令データの判断の結果、データファイル選択命令データであれば、制御素子15は、データメモリ16から本命令データ中のデータファイル名と同一のデータファイル名を持つアプリケーションデータファイルを見付ける。もし見付からなければ、制御素子15は、データファイル未定義を意味する応答データを出力し、命令データ待ち状態に戻る。

【0033】もし見付かれば、制御素子15は、図7のデータファイル名格納部24に本命令データ中のデータファイル名を格納し、かつ、照合状態格納部232の内容を未照合状態、すなわち、全てのビットを「0」とする。そして、制御素子15は、データファイル選択完了を意味する応答データを出力し、命令データ待ち状態に戻る。

【0034】ICカードの起動時には、図7の各格納部231，232，24の内容は全て「0」となっており、このとき、たとえば、データファイル名「×××」を有するデータファイル選択命令データが入力されると、データファイル名格納部24には「×××」という値が格納される。

【0035】次に、キーデータの照合処理を説明する。前記データファイル選択命令データか否かの判断の結果、データファイル選択命令データでなければ、制御素子15は、次に図10に示すようなキーデータ照合命令データか否かを判断する。この判断の結果、キーデータ照合命令データでなければ、制御素子15は別の処理を行なう。

【0036】上記命令データの判断の結果、キーデータ照合命令データであれば、制御素子15は、まず、データファイル名格納部24の内容が「0」となっているか否か（データファイルが選択されているか否か）を判断する。この判断の結果、もし「0」となっていれば、データファイルが何も選択されていないことになる。したがって、制御素子15は、コモンデータファイル21を参照することにより、本命令データ中の識別情報（KID）と同一の識別情報（KID）を持つキーデータを見付ける。

【0037】上記判断の結果、もし「0」となっていなければ、データファイルが選択されていることになる。したがって、制御素子15は、コモンデータファイル21、および、選択されたアプリケーションデータファイル221または222を参照することにより、同様に本命令データ中の識別情報と同一の識別情報を持つキーデータを見付ける。もし見付からなければ、制御素子15は、キーデータ未定義を意味する応答データを出力し、命令データ待ち状態に戻る。

【0038】もし見付かれば、制御素子15は、そのキーデータと本命令データ中のキーデータとを照合する。この照合の結果、両者が一致していれば、制御素子15は、このキーデータがコモンデータファイル21に属するか、アプリケーションデータファイル221，222に属するかを判断する。

【0039】この判断の結果、コモンデータファイル21に属するものであれば、制御素子15は、そのキーデータに付与されている照合状態指定情報を参照し、「1」となっているビットと同一の照合状態格納部231のビットを「1」にする。

【0040】また、アプリケーションデータファイル221，222に属するものであれば、制御素子15は、同様に、こんどは照合状態格納部232の同一ビットを「1」にする。そして、キーデータ一致を意味する応答データを出力し、命令データ待ち状態に戻る。

【0041】上記キーデータの照合の結果、両者が一致していなければ、制御素子15は、同様にして、照合状態格納部231あいるは照合状態格納部232の同一ビットを「0」にする。そして、キーデータ不一致を意味する応答データを出力し、命令データ待ち状態に戻る。

【0042】たとえば、データファイル選択命令データによりアプリケーションデータファイル222を選択した後、キーデータ1、キーデータY5およびY6を照合すると、照合状態格納部231の内容は「10000000」、照合状態格納部232の内容は「00001100」、また、データファイル名格納部24の内容は「YYY」となる。この後に、アプリケーションデータファイル221を選択すると、照合状態格納部231の内容は変化せず、照合状態格納部232の内容は「00000000」となり、また、データファイル名格納部24の内容は「×××」となる。

【0043】次に、エリア処理（エリア内データの読出、書込、消去）を説明する。前記キーデータ照合命令データか否かの判断の結果、キーデータ照合命令データでなければ、制御素子15は、次に図11（a）に示すような読出命令データ、図11（b）に示すような書込命令データ、あるいは、図11（c）に示すような消去命令データか否かを判断する。この判断の結果、図11のようなエリア処理命令データでなければ、制御素子15は別の処理を行なう。

【0044】上記命令データの判断の結果、エリア処理命令データであれば、制御素子15は、まず、データファイル名格納部24の内容が「0」となっているか否かを判断する。この判断の結果、もし「0」となっていれば、データファイルが何も選択されていないことにな

る。したがって、制御素子１５は、コモンデータファイル２１を参照することにより、本命令データ中の識別情報（ＡＩＤ）と同一の識別情報（ＡＩＤ）を持つエリアを見付ける。

【００４５】上記判断の結果、もし「０」となっていなければ、データファイルが選択されていることになる。したがって、制御素子１５は、コモンデータファイル２１、および、選択されたアプリケーションデータファイル２２１または２２２を参照することにより、同様に本命令データ中の識別情報と同一の識別情報を持つエリアを見付ける。もし見付からなければ、制御素子１５は、エリア未定義を意味する応答データを出力し、命令データ待ち状態に戻る。

【００４６】もし見付かれば、制御素子１５は、照合状態格納部２３１の内容と照合状態格納部２３２の内容との論理和をとり、その結果を「結果１」としておく。次に、制御素子１５は、本命令データ中の命令コードと同一の命令コードを図８のデータテーブルから検索することにより、各エリアに割当てられている２つの照合状態確認情報を選択する。たとえば、エリア処理命令データが読出命令データであれば、その命令コードが「ｚｚ」なので、それに対応する選択情報「１」により第１照合状態確認情報が選択され、書込命令データであれば、その命令コードが「ｗｗ」なので、それに対応する選択情報「２」により第２照合状態確認情報が選択され、消去命令データであれば、その命令コードが「ｖｖ」なので、それに対応する選択情報「２」により第２照合状態確認情報が選択される。

【００４７】このようにして、第１または第２照合状態確認情報を選択すると、制御素子１５は、その選択した照合状態確認情報を参照し、それに付与されている論理情報がアンド論理となっているか否かを判断する。この判断の結果、もしアンド論理でなければ（オア論理となっている）、制御素子１５は、照合状態確認情報の全てのビットが「０」か否かを判断する。この判断の結果、もし全てのビットが「０」であれば、制御素子１５は、照合状態を確認せずにエリアに対する処理を行なう。

【００４８】上記判断の結果、もしどれかのビットが「１」となっていれば、制御素子１５は、その「１」となっているビットに対応する前記結果１内のビットのどれかが「１」となっているか否かを判断する。この判断の結果、もしどのビットも「１」となっていなければ、制御素子１５は、アクセス不可を意味する応答データを出力し、命令データ待ち状態に戻る。上記判断の結果、もしどれか１つのビットでも「１」となっていれば、制御素子１５は、エリアに対する処理を行なう。

【００４９】上記論理情報の判断の結果、もしアンド論理になっていれば、制御素子１５は、同様に照合状態確認情報の全てのビットが「０」か否かを判断する。この判断の結果、もし全てのビットが「０」であれば、制御素子１５は、エリアへのアクセスが禁止されていると判断して、アクセス不可を意味する応答データを出力し、命令データ待ち状態に戻る。

【００５０】上記判断の結果、もしどれかのビットが「１」となっていれば、制御素子１５は、本照合状態確認情報と前記結果１とを比較する。この比較の結果、もし両者が一致していなければ、制御素子１５は、同様にアクセス不可を意味する応答データを出力し、命令データ待ち状態に戻る。上記比較の結果、もし両者が一致していれば、制御素子１５は、エリアに対する処理を行ない、その処理終了後、処理結果を応答データとして出力し、命令データ待ち状態に戻る。

【００５１】ここで、具体的に説明すると、図４の例において、たとえば、エリアＢについては、それに付与されている第１照合状態確認情報の論理情報がアンド論理（Ａ）で、第１照合状態確認情報報は「１０００００００」となっている。したがって、キーデータ１の照合のみが済んでいる状態でエリアＢへの読出しアクセスが可能となる。また、第２照合状態確認情報は「０００００００」で、その論理情報がオア論理（Ｏ）となっている。したがって、エリアＢへの書込みおよび消去アクセスは、キーデータの照合が不要であることを示している。

【００５２】また、エリアＣについては、第１照合状態確認情報は「００００００００」で、その論理情報がアンド論理（Ａ）となっている。したがって、エリアＣへの読出しアクセスは不可となる。また、第２照合状態確認情報は「００００１１００」で、その論理情報がオア論理（Ｏ）となっている。したがって、キーデータＸ５あるいはキーデータＸ６のどちらかの照合が済んでいれば、エリアＣへの書込みおよび消去アクセスは可能となる。

【００５３】また、キーデータＹ５およびキーデータＹ６の照合後、アプリケーションデータファイル２２１を選択してエリアＣへの書込みアクセスを実行すると、その選択時にキーデータＹ５およびキーデータＹ６の照合状態はクリアされるため、アクセスは不可となる。

【００５４】すなわち、このことから、アプリケーションデータファイル２２１，２２２内のキーデータの照合状態は、同一のアプリケーションデータファイル内のエリアへのアクセスに対してのみ有効となる。

【００５５】また、アプリケーションデータファイル２２１のキーデータＸ４とアプリケーションデータファイル２２２のキーデータＹ４とは同一の識別情報（ＫＩＤ）を与えられているが、識別情報の指定の際には、どちらか１つのアプリケーションデータファイルのみがアクセスの対象となっているため、混同することはない。ただし、コモンデータファイルと他のアプリケーションデータファイルとの間では同一の識別情報（ＫＩＤ）を使用しないようにする。なお、エリアに対して与える識

別情報（ＡＩＤ）についても同様である。

【００５６】また、同一のアプリケーションデータファイル内において、識別情報（ＡＩＤ）および識別情報（ＫＩＤ）については、命令データとしてどちらに対してアクセスするかが一義的に決まるため、同一の値を使用してもよい。

【００５７】さらに、各エリアに対して与えられる照合状態確認情報の数についても、エリアに対する命令および処理の数に対応して変更可能である。このように、データメモリ内に複数のキーデータ（暗証番号）を記憶しておき、これらキーデータを選択的に外部から入力されるキーデータと照合し、この照合結果を上記各キーデータごとに記憶しておき、データメモリのエリアに対してのアクセスの際、上記記憶してある各照合結果のうちいずれか１つが肯定的となっているときアクセス可能とし、上記記憶してある各照合結果の全てが肯定的となっているときアクセス可能とし、かつ、それらをデータメモリの各エリアに対するアクセスのための命令データごとに設定できるようにしている。

【００５８】これにより、データメモリの各エリアごとにエリアへのアクセスに必要となるキーデータの組合せを任意に設定でき、その組合せに対して特にアンド論理あるいはオア論理を合せて設定でき、かつ、その組合せはデータメモリの各エリアに対するアクセスのための命令データごとに設定できる。したがって、データメモリの各エリアへのアクセス条件がきめ細かく設定でき、ＩＣカードシステムの構築において柔軟性が得られるようになる。

【００５９】すなわち、ファイルごとにキーデータ（暗証番号）が記憶されているので、ファイルごとに異なるキーデータを用いることができる。また、ファイルごとのキーデータを用いてファイル内の各エリアのアクセス条件が記憶されているので、ファイルごと、および、エリアごとにアクセス条件を変えることができる。さらに、ファイルを選択していないとキーデータの照合が不可能となるので、キーデータの漏洩を防止することが＊できる。

【００６０】

【発明の効果】以上詳述したように本発明によれば、ファイルごとに異なる認証情報を用いることができるとともに、ファイルごと、および、エリアごとにアクセス条件を変えることができ、しかも、認証情報の漏洩を防止することができる携帯可能電子装置および携帯可能電子装置におけるアクセス管理方法を提供できる。

【図面の簡単な説明】

【図１】各処理動作を説明するフローチャート。

【図２】各処理動作を説明するフローチャート。

【図３】各処理動作を説明するフローチャート。

【図４】データメモリのファイル構造を示す図。

【図５】キーデータに対する諸情報を説明する図。

【図６】エリアに対する諸情報を説明する図。

【図７】照合状態格納部およびデータファイル名格納部を説明する図。

【図８】各種命令コードに対応して照合状態確認情報を選択するための選択情報が格納されているデータテーブルを説明する図。

【図９】データファイル選択命令データのフォーマット例を示す図。

【図１０】キーデータ照合命令データのフォーマット例を示す図。

【図１１】エリアへの読出命令データ、書込命令データ、および、消去命令データのフォーマット例を示す図。

【図１２】ＩＣカードの構成を示すブロック図。

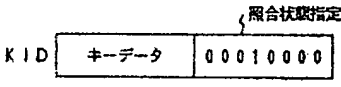
【図１３】ＩＣカードの機能ブロックを示す図。

【図１４】端末装置の構成を示すブロック図。

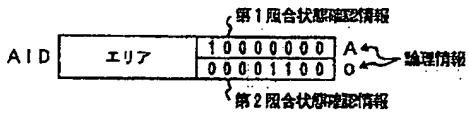
【符号の説明】

１……ＩＣカード（携帯可能電子装置）、１５……制御素子（制御部）、１６……データメモリ（メモリ部）、１７……プログラムメモリ、２１……コモンデータファイル、２２１，２２２……アプリケーションデータファイル、２３１，２３２……照合状態格納部。

【図５】

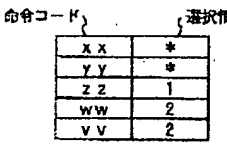


【図６】

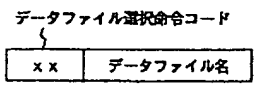


【図７】

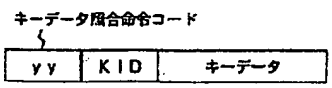
【図８】



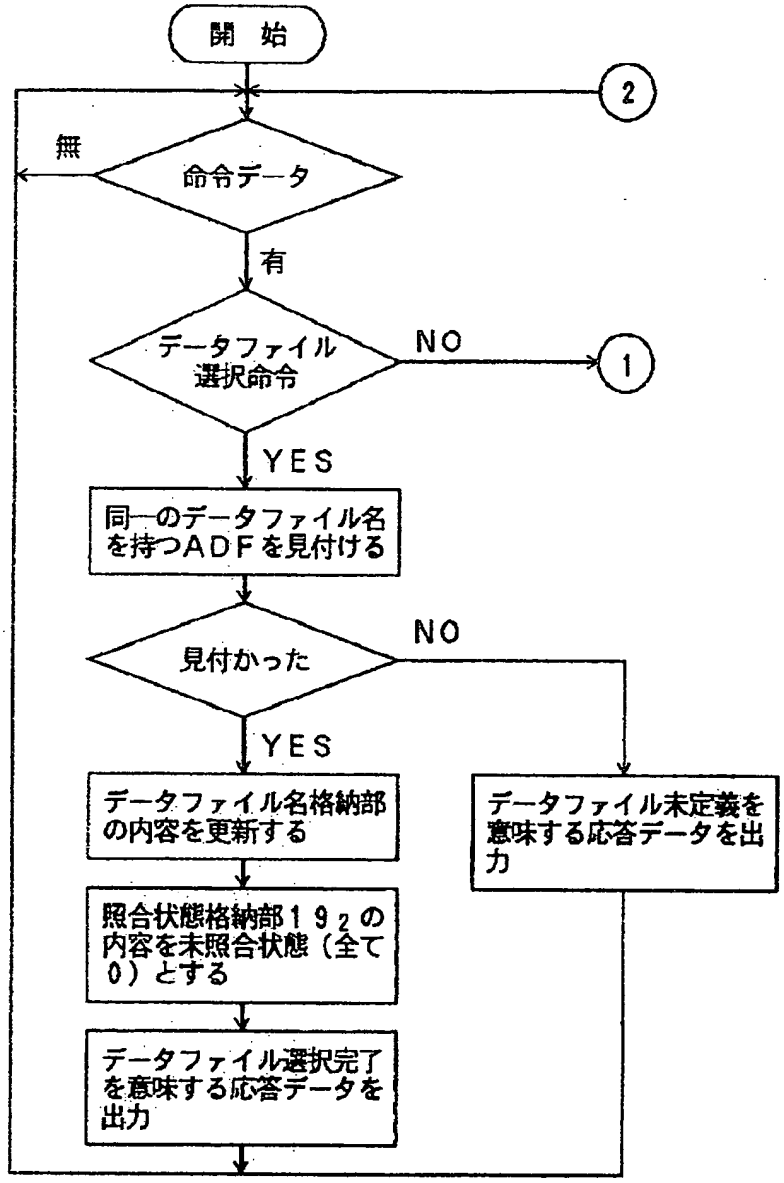
【図９】



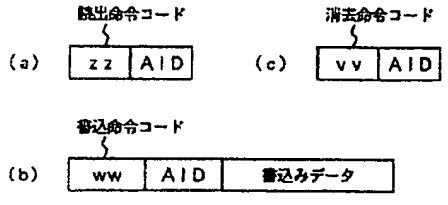
【図１０】



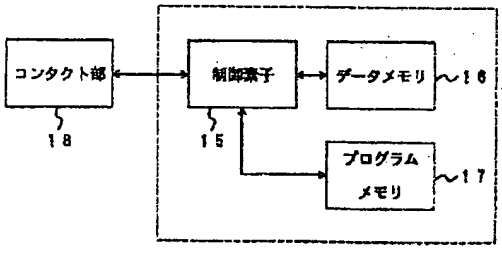
【図１】


開　始
2
無
命令データ
有
データファイル
選択命令
NO
1
YES
同一のデータファイル名
を持つＡＤＦを見付ける
見付かった
NO
YES
データファイル名格納部
の内容を更新する
データファイル未定義を
意味する応答データを出
力
照合状態格納部１９２の
内容を未照合状態（全て
０）とする
データファイル選択完了
を意味する応答データを
出力

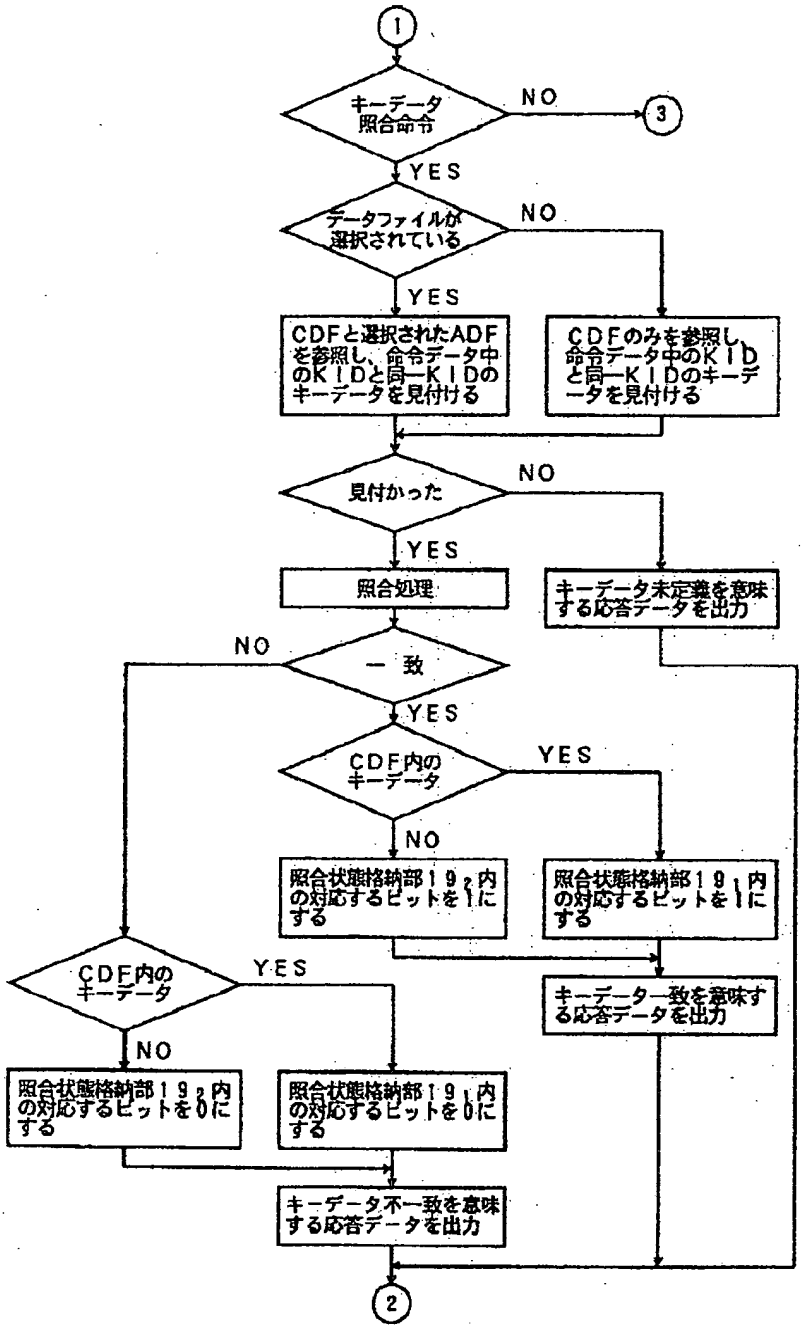
【図１１】


読出命令コード
(a)
zz
AID
消去命令コード
(c)
vv
AID
書込命令コード
(b)
ww
AID
書込みデータ

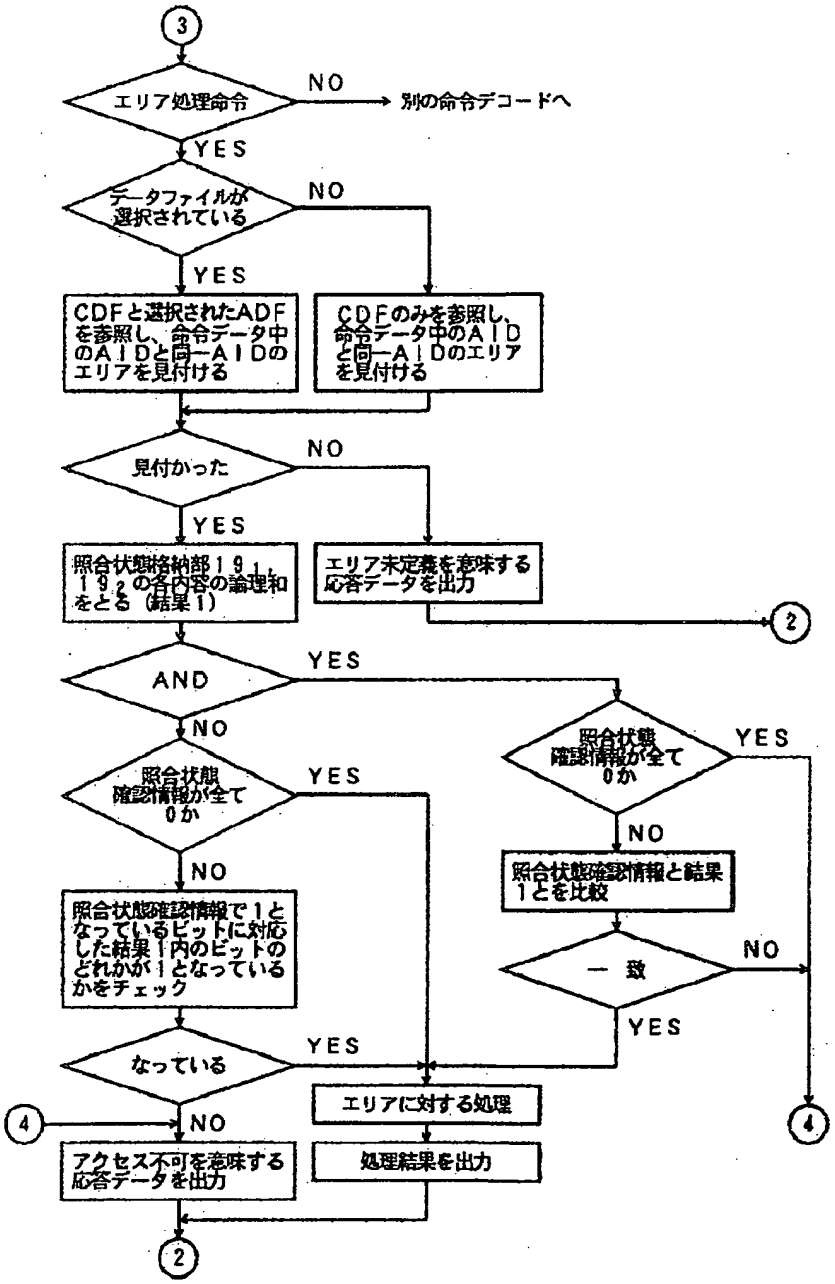
【図１２】


コンタクト部
18
制御素子
15
データメモリ
16
プログラム
メモリ
17

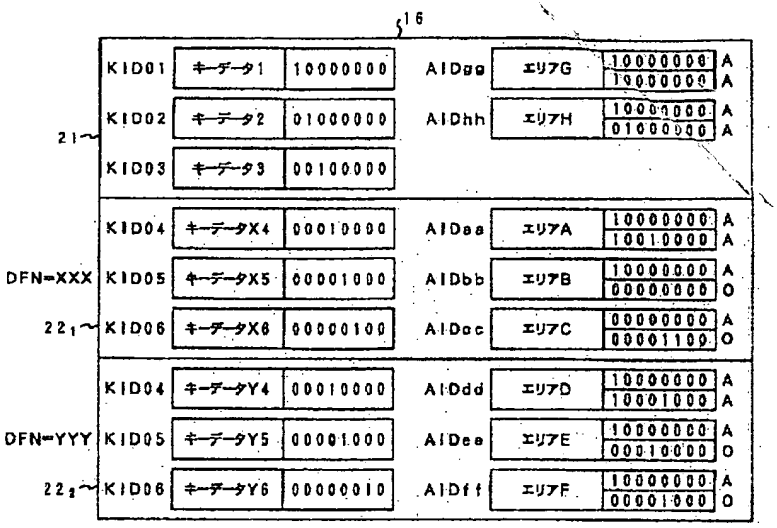
【図２】


①
キーデータ照合命令
NO
③
YES
データファイルが選択されている
NO
YES
CDFと選択されたADFを参照し、命令データ中のＫＩＤと同一ＫＩＤのキーデータを見付ける
CDFのみを参照し、命令データ中のＫＩＤと同一ＫＩＤのキーデータを見付ける
見付かった
NO
YES
照合処理
キーデータ未定義を意味する応答データを出力
NO
一致
YES
CDF内のキーデータ
YES
NO
照合状態格納部１９２内の対応するビットを１にする
照合状態格納部１９１内の対応するビットを１にする
CDF内のキーデータ
YES
キーデータ一致を意味する応答データを出力
NO
照合状態格納部１９２内の対応するビットを０にする
照合状態格納部１９１内の対応するビットを０にする
キーデータ不一致を意味する応答データを出力
②

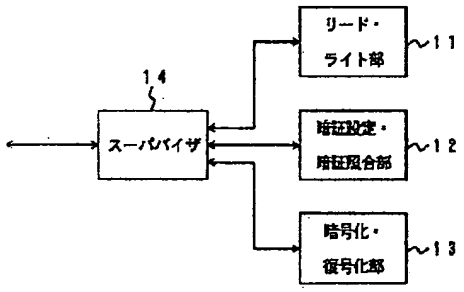
【図３】


3
エリア処理命令
NO
別の命令デコードへ
YES
データファイルが選択されている
NO
YES
CDFと選択されたADFを参照し、命令データ中のＡＩＤと同一ＡＩＤのエリアを見付ける
CDFのみを参照し、命令データ中のＡＩＤと同一ＡＩＤのエリアを見付ける
見付かった
NO
YES
照合状態格納部１９１，１９２の各内容の論理和をとる（結果１）
エリア未定義を意味する応答データを出力
2
AND
YES
NO
照合状態確認情報が全て0か
YES
NO
照合状態確認情報が全て0か
YES
NO
照合状態確認情報と結果１とを比較
照合状態確認情報で１となっているビットに対応した結果１内のビットのどれかが１となっているかをチェック
一 致
NO
YES
なっている
YES
4
NO
エリアに対する処理
処理結果を出力
アクセス不可を意味する応答データを出力
4
2

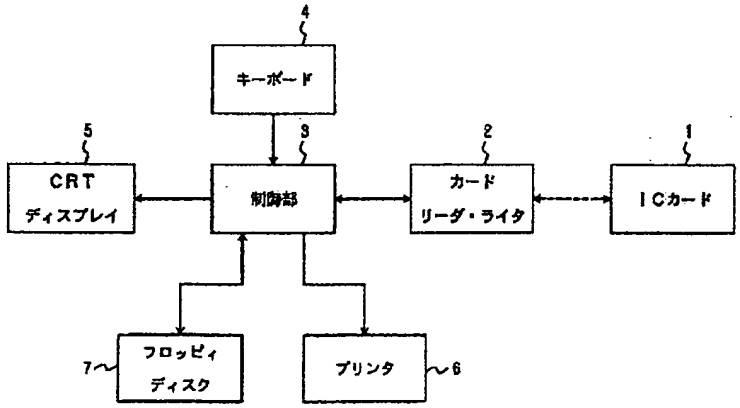
【図4】


16
21
KID01
キーデータ1
10000000
AIDgg
エリアG
10000000 A
10000000 A
KID02
キーデータ2
01000000
AIDhh
エリアH
10000000 A
01000000 A
KID03
キーデータ3
00100000
DFN=XXX
KID04
キーデータX4
00010000
AIDaa
エリアA
10000000 A
10010000 A
KID05
キーデータX5
00001000
AIDbb
エリアB
10000000 A
00000000 O
22₁
KID06
キーデータX6
00000100
AIDcc
エリアC
00000000 A
00001100 O
DFN=YYY
KID04
キーデータY4
00010000
AIDdd
エリアD
10000000 A
10001000 A
KID05
キーデータY5
00001000
AIDee
エリアE
10000000 A
00010000 O
22₂
KID06
キーデータY6
00000010
AIDff
エリアF
10000000 A
00001000 O

【図13】


14
スーパバイザ
リード・
ライト部
11
暗証設定・
暗証照合部
12
暗号化・
復号化部
13

【図14】


4
キーボード
5
CRT
ディスプレイ
3
制御部
2
カード
リーダ・ライタ
1
ICカード
7
フロッピィ
ディスク
プリンタ
6